VA Software Assurance

Office of Information Security

Secure Coding Tips

Tip: An Abridged Secure Code Review Validation Preparation Checklist

This week's Secure Coding Tip is an abridged secure code review validation preparation checklist, items that are recommended to double-check before requesting a validation. Scanning source code to perform code review is an authorization requirement included in the Technical / Testing Requirements of the OCS Accreditation Requirements Guide / SOP [1] , and enforced as part of the ATO issuance process.[2]

The following items are recommended to make sure there are no issues with before requesting a validation:

- Check that the scan matches the source code
- Check that there are no scan errors
- Check that the filter set is "Security Auditor View"
- Check that there are no remaining critical findings
- Check that there are no remaining high findings
- Check that false positives are explained in comments
- Check that no findings have been suppressed
- Check that any custom rule files are also provided

Read more...

[1] "Accreditation Requirements Guide / Standard Operating Procedures", Office of Cyber Security (OCS) Assessment and Authorization intranet site.

[2] "Accreditation Requirements Expectation Memorandum" (Section 2.a.ii "Code Review"), VA Chief Information Security Officer (CISO) Stanley F. Lowe, March 19, 2014.

More Information

For more information about the VA Software Assurance Program Office, please visit our website here.

Resources

VA Software Assurance Support Site

VA Code Review Standard Operating Procedures

VA Code Review Process eLearning Module

VA-Licensed Fortify Request Instructions

VA Software Assurance Training Schedule

VA Software Assurance Frequently Asked Questions

Next Class:

7/27